LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of preventing ID spoofing of public key infrastructure system in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate.; and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

2. (Original) The method of claim 1, further comprising providing user identifiers and their corresponding digital signature certificates in said directory.

3. (Original) The method of claim 1, further comprising providing an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

4. (Original) The method of claim 1, further comprising providing a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize a user.

5. (Currently Amended) A method of preventing ID spoofing of a public key infrastructure in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that a signature certificate will not be issued, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate; and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

6. (Original) The method of claim 5, further comprising providing user identifiers and their corresponding digital signature certificates in said directory.

7. (Original) The method of claim 5, further comprising providing an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

8. (Original) The method of claim 5, further comprising providing a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize the user.

9. (Currently Amended) An apparatus for preventing ID spoofing of a public key infrastructure system in an enterprise comprising: a registration server to allow access by a user; a directory accessible by the registration server, the directory storing information regarding all users in the enterprise; wherein, upon the registration server receiving information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user; and wherein, upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate, such that the directory maintains a one-to-one correspondence between the users of the enterprise and signature certificates.

10. (Original) The apparatus of claim 9, wherein the directory includes identifiers and their corresponding digital signature certificates.

11. (Original) The apparatus of claim 9, further comprising an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

12. (Original) The apparatus of claim 9, further comprising a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize a user.

13. (Currently Amended) An apparatus for preventing ID spoofing of a public key infrastructure in an enterprise comprising: a registration server to allow access by a user; a directory accessible by the registration server, the directory storing information regarding all users in the enterprise; wherein, upon the registration server receiving information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user; and wherein, upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that the user is not a valid member of the enterprise and not issue a signature certificate~~.~~, such that the directory maintains a one-to-one correspondence between the users of the enterprise and signature certificates.

14. (Currently Amended) The apparatus of claim ~~12~~13, wherein the directory includes identifiers and their corresponding digital signature certificates.

15. (Currently Amended) The apparatus of claim ~~12~~13, further comprising an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

16. (Currently Amended) The apparatus of claim ~~12~~13, further comprising a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize the user.